Instructions for Keeping the Online Security Center up to date

Background

The OSC was introduced to the FSA community in January 2004. It has revolutionized the communication within FSA and enabled the SSOs to do their job more effectively and efficiently. One key to making this web portal useful is its timeliness. The SSOs expect the web portal to have the latest versions of the documentation, etc. The OSC must be updated frequently (at least once a week, if not more) in order to maintain its usefulness. The website address is http://fsanet.ed.gov/cio/products/it_security_portal/.

Updates

To update the OSC, you must email your changes to FSAnet. You can do this in one of two ways:

1. Email the changes through Outlook directly to the FSAnet Content Box. In the "To" field, type FSA Net Content and the address will automatically come up or you can type the exact email address: FSA_Net_Content@ed.gov.

2. The second option is in Outlook, under the Tools tab, choose Forms, and then Choose Form. Once there choose the FSA Net Content form. Just fill in the blanks on the form and it will automatically come to our FSAnet Content Box. Fill out your phone number, Channel/Area is CIO, priority is usually low, and then attach the docs in the content box.

The point of contact is Jerome Davis.
Updates are usually made within a day or two after they are sent out.

Calendar

Every month, prepare a calendar of events like the sample included in Appendix A. In the calendar, there are events for training, workshops, and any other relevant event. Also include important events from the Department or FSA in the calendar; this would include things like SSO meetings. The calendar is primarily based on a series of websites, including:

- http://csrc.nist.gov/events/index.html
- http://www.fcw.com/agenda.asp
- http://www.net-security.org/webcasts.php
- http://www.iacr.org/events/
- http://www.ioss.gov/calendar.html
- www.microsoft.com webcasts

Send the calendar for the next month approximately three days before the end of the month in order to give the FSAnet programmers sufficient time to prepare the calendar.

Security News

Security News is just what it says, events in the security world that would be of interest to FSA. This is usually updated at least once a week, preferably daily. The events are usually taken from articles from this site:
http://news.ists.dartmouth.edu/todaysnews.html#internal14298

What's Hot

What's Hot is a section about whatever is going on that is important. It could be another news article, or it could have something to do with whatever is going on in FSA, like announcing an SSO meeting.

Tip of the Month

This is naturally updated once a month at the beginning of the month. Send it to the FSAnet programmers at least a day in advance before the new month starts. The content can be anything that is worth highlighting that will help the SSOs do their job better or provide them with further education.

Staff Directory

Approximately on a monthly basis, the FSA CSO will issue an updated SSO list. The OSC webmistress must compare that list to the Staff Directory online (under Help Desk) and send any updates to the Directory in.

Document updates

FSA, like any agency, has policy changes. There are a number of documents on the OSC. Some of these documents are in two places. For instance, under Security Front to Back, under Incident Response, one of the FSA documents is the FSA Incident Implementation Guide. This same guide is also under Policies/Regulations, under FSA policies. When policies are updated, they must be synchronized in all of the places where they are located, otherwise people will get confused regarding versions.

Appendix A- Calendar sample

Date:		June 2, 2004
Event:	Webcast	Patch Management
Description of Event:		This webcast will cover the following topics: Introduction to the NIST 800-40 document as an industry best practices document for conducting patch management; Creation of a Patch and Vulnerability Group; Assigning responsibilities; Finding vulnerability and patch information; Evaluating patches; Types of products available including commercial and free tools as well as agent based versus network based; Selection criteria for choosing a product and Alternative mitigation techniques.
Cost:		Free
Time:		1 P.M.
Website:		http://www.sans.org/webcasts/show.php?webcastid=90477
Date:		June 2, 2004
Event:	Webcast	Sophos Anti-Virus: Stopping viruses in the educational environment
Location:		Online
Description of Event:		Sophos Anti-Virus is the leading anti-virus solution for the education sector, protecting more than 1200 K-12 and post-secondary institutions, including Harvard, New York University, Texas Tech, and UCLA. In this free, 1-hour web seminar, Korey Ferland, Product Marketing Manager, shows how Sophos provides a high performance, cost effective anti-virus solution for the educational institution. Specific examples from these leading institutions will be provided: The Open University (OU) - The UK's largest university, with more than 200,000 students, many of whom study interactively over the internet. SAV is currently deployed on servers in 13 UK offices and one in Brussels. It protects 7000 machines belonging to academic and administrative staff at the university's main site, regional offices, and at home. Harrison School District Two (HSD2) - Colorado Spring's

		Harrison School District Two is a network of 19 schools with two administrative sites and 10,500 students. HSD2's vulnerability to viruses increased when students were given internet access. Since implementing Sophos Anti-Virus, the district's staff has significantly reduced the time spent dealing with virus issues
Time:		10 am- 11 am
Website:		http://www.net-security.org/webcast.php?id=283
Cost:		Free
Registration:		https://activestateevents.webex.com/sophos/onstage/framesets/register.php?ConfID=277154990&Rnd=210011968
Date:		June 3, 2004
Event:	Briefing	NIST 800-37 Briefing
Venue:		Green Auditorium
Location:		NIST Main Campus, Gaithersburg, Maryland.
Description of Event:		NIST is pleased to announce a Briefing Day for Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems." The purpose of the Briefing Day is to provide federal agencies with the latest information on the implementation of NIST Special Publication 800-37. The target audience for the briefing day is Chief Information Officers (CIO), Senior Agency Information Security Officers (SAISO), and Inspectors General (IG). In addition to detailed presentations on the NIST FISMA project and Special Publication 800-37, representatives from OMB will be in attendance to provide the latest policy guidance on the implementation of the special publication. Attendance at the Briefing Day is by invitation ONLY and limited to federal employees holding CIO, SAISO, or IG positions. The number of participants is limited to three per agency or major organizational component. Participants must be pre-registered.
Cost:		Free
Registration:		Electronic registration may be done at: http://www.nist.gov/conferences, click on View Upcoming NIST Conferences, and then scroll down to the June 3, 2004 Briefing Day.
Time:		9:00 A.M. until 12:30 P.M. in the